



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR    | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|-----------------|-------------|-------------------------|---------------------|------------------|
| 09/893,461      | 06/29/2001  | Michael Thomas Kurdziel | HAR65 001           | 6363             |

7590 03/24/2005

DUANE MORRIS LLP  
1667 K STREET NW  
SUITE 700  
WASHINGTON, DC 20006

EXAMINER

BROWN, CHRISTOPHER J

|          |              |
|----------|--------------|
| ART UNIT | PAPER NUMBER |
|----------|--------------|

2134

DATE MAILED: 03/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

|                              |  |   |  |
|------------------------------|--|---|--|
| <b>Office Action Summary</b> | <b>Application No.</b><br>09/893,461   | <b>Applicant(s)</b><br>KURDZIEL, MICHAEL THOMAS |  |
|                              | <b>Examiner</b><br>Christopher J Brown | <b>Art Unit</b><br>2134                         |  |

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) ☒ Responsive to communication(s) filed on 04 June 2002.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☒ Claim(s) 4,6,8 and 10 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 29 June 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

- |   |   |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)   | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)  | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date <u>10/01/2001</u> . | 6) <input type="checkbox"/> Other: _____  |

*7/2*

## **DETAILED ACTION**

### ***Claim Objections***

1. Claim 4 is objected to because of the following informalities: The claim lacks a transitional phrase. Appropriate correction is required.

Claim 4 is objected to because of the following informalities: line 8 consists of the sentence "...the operation of the most downstream of the modulo operators ...". The examiner assumes that the sentence should read "...the operation of most downstream modulo operators...". Appropriate correction is required.

Claim 4 is objected to because of the following informalities: The claim's first line is grammatically incorrect. Appropriate correction is required.

Claim 6 is objected to because of the following informalities: The claim's first line is grammatically incorrect. Appropriate correction is required.

Claim 6 is objected to because of the following informalities: The claim lacks a transitional phrase. Appropriate correction is required.

Claim 8 is objected to because of the following informalities: The claim's first line is grammatically incorrect. Appropriate correction is required.

Claim 10 is objected to because of the following informalities: The claim depends on a non-existent "Claim 11" Appropriate correction is required.

***Claim Rejections - 35 USC § 112***

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

Claims 1, 4, 6, 7, and 8 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The use of the word "responsive" is vague and indefinite. The examiner recommends a more descriptive word, or phrase regarding the invention.

Claim 1 recites the limitations "first block cipher" and "second block cipher" in lines 8 and 9. There is insufficient antecedent basis for this limitation in the claim. The examiner recommends amending the description of the previously stated block ciphers in claim 1.

Claim 4 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as

the invention. Claim 4 states on lines 6 and 7 “a block cipher device having the second key for operation with a block cipher device having the second key...” The examiner believes one of these “second keys” was intended to be a “first key” Appropriate correction is required.

Claim 6 recites the limitation "symbols" in line 10. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 recites the limitation "the improvement" in line 4. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 recites the limitation "the serial output" in line 9. There is insufficient antecedent basis for this limitation in the claim.

Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being incomplete for omitting essential steps, such omission amounting to a gap between the steps. See MPEP § 2172.01. The omitted steps are: Providing for the shift register to produce a serial output.

Claim 8 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Lines 16-18 virtually duplicate lines 9-11, and on line 16 “a first modulo two summing combiner” is repeated from line 9. The examiner believes that lines 16-18 should be directed towards the second shift register.

Claims 2, 3, 5, 9 and 10 are rejected based on their dependence on rejected independent claims.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 4 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore US 6,061,449 in view of Coutts US 5,835,603.

As per claims 1, 4, and 6 Candelore teaches using a public/private key algorithm in a block cipher encryption/ decryption system, (Col 32 lines 1-15). Candelore does not specifically teach using a fixed length set of keys.

Coutts teaches using fixed length keys with various well known cryptographic algorithms, (Col 3 lines 34-38).

It would have been obvious to one skilled in the art to use the teachings of Coutts with Candelore because the algorithms taught in Coutts are well known and secure.

Art Unit: 2134

Claims 2-3 are rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore US 6,061,449 in view of Coutts US 5,835,603 in view of Matyas US 5,201,000

As per claims 2, 3, and 5 The previous Candelore-Coutts combination does not teach specified key length.

Matyas teaches using an algorithm to generate a key pair of whatever bit length is desired, (col 14 lines 8-13).

It would have been obvious to generate different but key lengths based on the public private key algorithm in Candelore-Coutts.

Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Candelore US 6,061,449 in view of Coutts US 5,835,603 in view of Lim US 2002/0018562

The previous Candelore-Coutts combination does not teach a key scheduler.

Lim teaches a key scheduler generating two subkeys, [0031].

It would have been obvious to one skilled in the art to use the teachings of Lim with the system of Candelore-Coutts because the key scheduler generates a plurality of keys.

### ***Conclusion***

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Christopher J Brown whose telephone number is (571)272-3833. The examiner can normally be reached on 8:30-6:00.

Art Unit: 2134

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571)272-3838. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Christopher J Brown

3/11/05



GREGORY MORSE  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100